

REMARKS/ARGUMENTS

Favorable reconsideration of this application, in light of the following discussion, is respectfully requested.

Claims 1-78 are pending in the present application.

In the outstanding Office Action, Claims 1, 6, 7, 15, 29, and 38 were rejected under 35 U.S.C. §103(a) as unpatentable over Deville et al., *Interoperability Issues of Existing Collateral Video Teleconferencing Systems at the United States Pacific Command, Military Communications Conference*, 1994, MILCOM '94, Conference: Record, 1994 IEEE Fort Monmouth, N.J., USA 2-5 Oct. 1994, New York, N.Y., USA, IEEE, US, Xp010149676 (hereinafter Deville) in view of Lauper et al. (U.S. Patent No. 6,717,607, hereinafter Lauper); Claims 2, 5, and 8 were rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Seamaan (U.S. Patent No. 5,680,392); Claim 3 was rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Raike et al. (U.S. Patent No. 7,076,067, hereinafter Raike); Claim 4 was rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Mulford (U.S. Patent No. 5,301,232); Claim 9 was rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Voois et al. (U.S. Patent No. 6,124,882, hereinafter Voois); Claim 10 was rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Boundy (U.S. Patent No. 6,981,022); Claim 11 was rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of Fernandez et al. (U.S. Patent No. 6,590,602, hereinafter Fernandez); Claims 12-14 were rejected under 35 U.S.C. §103(a) as unpatentable over Deville in view of Lauper, and further in view of in view of Ragunathan et al. (U.S. Patent Publication No. 2003/0142818, hereinafter Ragunathan); Claims 47 and 77 were rejected under 35 U.S.C. §102(b) as anticipated by Deville; Claims 48 and 49 were rejected

under 35 U.S.C. §103(a) as unpatentable over Denville in view of Nishizawa JP 408046723); Claims 50-56, 60-67, and 70-76 were rejected under 35 U.S.C. §103(a) as unpatentable over Denville in view of Lauper; Claims 58, 59, 68, 69, and 78 were rejected under 35 U.S.C. §103(a) as unpatentable over Denville in view of Lauper, and further in view of Nishizawa.

With respect to the rejection of Claim 1 as unpatentable over Denville in view of Lauper, Applicant respectfully traverses this ground of rejection. Claim 1 recites, *inter alia*,

A multi-protocol interface device, comprising...

...each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol...and

a video conference management data archive connected to the secure interface and configured to hold the link-unique encryption keys, wherein

said multi-protocol, video conference interface device is one of a gateway device and a multi-point control unit (MCU) device.

Page 3 of the outstanding Office Action concedes that Denville does not specifically teach these features of Claim 1. The outstanding Office Action relies on Lauper to cure the deficiencies in Denville.

Denville describes a VTC system than includes an MCU, wherein there is a bank of encryption units connected to the MCU. The encryption units of Denville are not built into the MCU. On the contrary, the encryption units are external to the MCU. Page 100, right column, of Denville states "...VTC data processed by MCUs must be in the clear, therefore, secure conferencing incorporating MCUs require an encryption device for each MCU communication port." Denville suggest that the encryption devices operate in pairs, one at the MCU and a corresponding one at the endpoint. These two corresponding encryption devices are interoperable with each other. However, in Denville, this requires a specific setup to ensure the interoperability of the two encryption devices, which is not expandable to have

interoperability with multiple devices, and will only use the encryption key that is included in the encryption device.

Lauper describes reducing bandwidth usage with at least three endpoints in a video conference call. Lauper only provides a brief description of a system using encryption modules to provide privacy in a videoconference. Lauper describes that central device 30 receives compressed and/or encrypted data and has a coding module 31 which decompresses and/or decrypts the data.<sup>1</sup> Lauper states “In the transmission of data from the central unit 30 to a communications unit 20, the coding module 31 also undertakes the compression and/or encryption of the data for the transmission.”<sup>2</sup>

Lauper does not disclose or suggest that central device 30 can encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol. The invention defined by Claim 1 has the functionality to use one of two encryption protocols. Lauper is silent as to whether central device 30 is configured to use one of two encryption protocols. The assertion that central device 30 uses one of two encryption protocols is merely speculative. While Fig. 1 of Lauper shows different links between the endpoints and central device 30, this does not mean that different encryption protocols are used.

Furthermore, Lauper does not disclose or suggest that central unit 30 is configured to hold the link-unique encryption keys. There is no disclosure or suggestion in Lauper that plural encryption keys are stored by central device 30. While the Office Action takes the position that this is implicit in Lauper, it is not necessarily so because the central device 30 may only use one key. There is not disclosure or suggestion in Lauper to have keys corresponding to a link-unique encryption protocol and a common encryption protocol.

---

<sup>1</sup> Lauper, col. 5, lines 39-41.

<sup>2</sup> Lauper, col. 5, lines 46-49.

Thus, Lauper does not disclose or suggest the claimed “each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol” and “a video conference management data archive connected to the secure interface and configured to hold the link-unique encryption keys.”

As Deville and Lauper do not disclose or suggest the claimed “each encryption device configured to encrypt with a link-unique encryption key corresponding to one of a common encryption protocol and a link-unique encryption protocol” and “a video conference management data archive connected to the secure interface and configured to hold the link-unique encryption key,” Applicant respectfully submits that a person of ordinary skill in the art could not properly combine Deville and Lauper to arrive at the invention defined by Claim 1.

In view of the above-noted distinctions, Applicant respectfully submits that Claim 1 (and any claims dependent thereon) patentably distinguish over Deville and Lauper, taken alone or in proper combination. Claims 15, 29, and 38 recite elements analogous to those of Claim 1. Thus, Applicant respectfully submits that Claims 15, 29, and 38 (and any claims dependent thereon) patentably distinguish over Deville and Lauper, taken alone or in proper combination, for at least the reasons stated for Claim 1.

With respect to the rejection of Claim 47 as anticipated by Deville, Applicant respectfully traverses this ground of rejection. Claim 47 recites, *inter alia*, “re-encrypting and relaying the first set of data from the interface device to a second terminal over a second communication link having a second communication protocol, the second communication protocol different from the first communications protocol.” Deville does not disclose or suggest this element of Claim 47.

Deville describes using the H.320 standard. There is no disclosure or suggestion that the MCU, with the external encryption devices, uses multiple communication protocols. Page 99, left column, states that "a solution to these issues is to (1) use identical CODECs from one manufacturer or specify use of a CODEC meeting the ITU Px64 (FIPS 178) standard." Page 99, right column, states "...digital couplinig requires that the two VTC systems being interconnected be operated at the same transmission rate with compatible CODECs at the end sites." Thus, the system described in the first partial paragraph in the left column of page 100 of Deville describes system that uses only one CODEC (H.320 or Px64).

Thus, Deville does not disclose or suggest the claimed "re-encrypting and relaying the first set of data from the interface device to a second terminal over a second communication link having a second communication protocol, the second communication protocol different from the first communications protocol."

In view of the above-noted distinctions, Applicant respectfully submits that Claim 47 (and any claims dependent thereon) patentably distinguish over Deville. Claim 77 recites elements that are similar to those of Claim 47. Thus, Applicant respectfully submits that Claim 77 patentably distinguish over Deville, for at least the reasons stated for Claim 47.

Consequently, in light of the above discussion, the present application is believed to be in condition for allowance and an early and favorable action to that effect is respectfully requested.

Respectfully submitted,

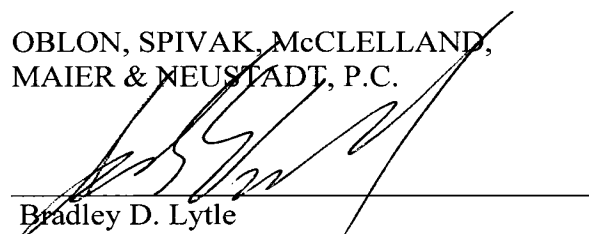
OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Customer Number

**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/07)

I:\ATTY\JWW\243610US\AMENDMEN1.DOC



---

Bradley D. Lytle  
Attorney of Record  
Registration No. 40,073  
Joseph Wrkich  
Registration No. 53,796